PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 17 June 1999 (17.06.99)	
International application No. PCT/NL98/00581	**Applicant's or agent's file reference** BO 41539 YK
International filing date (day/month/year) 09 October 1998 (09.10.98)	**Priority date** (day/month/year) 10 October 1997 (10.10.97)
Applicant DE LA BRETONIERE, Ralph, Rogier	

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International Preliminary Examining Authority on:

   07 May 1999 (07.05.99)

   [ ] in a notice effecting later election filed with the International Bureau on:

   _____

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

F. Baechler

Telephone No.: (41-22) 338.83.38

P NT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
BO 41539 YK		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/NL 98/ 00581	09/10/1998	10/10/1997
Applicant		
DE LA BRETONIERE, Ralph, Rogier		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 1

   [X] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

PCT

30. 11. 98

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT/NL 98 / 00581
International Application No.

09 OCT 1998
International Filing Date

09. 10. 98

BUREAU VOOR DE INDUSTRIËLE EIGENDOM
P.C T. INTERNATIONAL APPLICATION
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference
(if desired) (12 characters maximum) BO 41539 YK

Box No. I TITLE OF INVENTION

Method and device for protecting data communication

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

DE LA BRETONIÈRE, Ralph Rogier
Bijhouwerlommer 43
NL-2728 JK ZOETERMEER
The Netherlands

[X] This person is also inventor.

Telephone No.

Facsimile No.

Teleprinter No.

State *(that is, country)* of nationality: The Netherlands (NL)

State *(that is, country)* of residence: The Netherlands (NL)

This person is applicant for the purposes of: [X] all designated States [ ] all designated States except the United States of America [ ] the United States of America only [ ] the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:

[ ] applicant only

[ ] applicant and inventor

[ ] inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: [ ] all designated States [ ] all designated States except the United States of America [ ] the United States of America only [ ] the States indicated in the Supplemental Box

[ ] Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: [X] agent [ ] common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

DE BRUIJN, Leendert C. et al
Nederlandsch Octrooibureau
Scheveningseweg 82, P.O. Box 29720
NL-2502 LS The Hague
THE NETHERLANDS

Telephone No.
70 3527500

Facsimile No.
70 3527528

Teleprinter No.

[ ] **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent

Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent

- ☒ **AP** **ARIPO Patent:** **GH** Ghana, **GM** Gambia, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **SD** Sudan, **SZ** Swaziland, **UG** Uganda, **ZW** Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☒ **EA** **Eurasian Patent:** **AM** Armenia, **AZ** Azerbaijan, **BY** Belarus, **KG** Kyrgyzstan, **KZ** Kazakhstan, **MD** Republic of Moldova, **RU** Russian Federation, **TJ** Tajikistan, **TM** Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ **EP** **European Patent:** **AT** Austria, **BE** Belgium, **CH and LI** Switzerland and Liechtenstein, **CY** Cyprus, **DE** Germany, **DK** Denmark, **ES** Spain, **FI** Finland, **FR** France, **GB** United Kingdom, **GR** Greece, **IE** Ireland, **IT** Italy, **LU** Luxembourg, **MC** Monaco, **NL** Netherlands, **PT** Portugal, **SE** Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☒ **OA** **OAPI Patent:** **BF** Burkina Faso, **BJ** Benin, **CF** Central African Republic, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroon, **GA** Gabon, **GN** Guinea, **ML** Mali, **MR** Mauritania, **NE** Niger, **SN** Senegal, **TD** Chad, **TG** Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* .....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

- ☒ **AL** Albania
- ☒ **AM** Armenia
- ☒ **AT** Austria
- ☒ **AU** Australia
- ☒ **AZ** Azerbaijan
- ☒ **BA** Bosnia and Herzegovina
- ☒ **BB** Barbados
- ☒ **BG** Bulgaria
- ☒ **BR** Brazil
- ☒ **BY** Belarus
- ☒ **CA** Canada
- ☒ **CH and LI** Switzerland and Liechtenstein
- ☒ **CN** China
- ☒ **CU** Cuba
- ☒ **CZ** Czech Republic
- ☒ **DE** Germany
- ☒ **DK** Denmark
- ☒ **EE** Estonia
- ☒ **ES** Spain
- ☒ **FI** Finland
- ☒ **GB** United Kingdom
- ☒ **GE** Georgia
- ☒ **GH** Ghana
- ☒ **GM** Gambia
- ☒ ~~**GW** Guinea-Bissau~~
- ☒ **HR** Croatia
- ☒ **HU** Hungary
- ☒ **ID** Indonesia
- ☒ **IL** Israel
- ☒ **IS** Iceland
- ☒ **JP** Japan
- ☒ **KE** Kenya
- ☒ **KG** Kyrgyzstan
- ☒ **KP** Democratic People's Republic of Korea
- ☒ **KR** Republic of Korea
- ☒ **KZ** Kazakhstan
- ☒ **LC** Saint Lucia
- ☒ **LK** Sri Lanka
- ☒ **LR** Liberia
- ☒ **LS** Lesotho
- ☒ **LT** Lithuania
- ☒ **LU** Luxembourg
- ☒ **LV** Latvia
- ☒ **MD** Republic of Moldova
- ☒ **MG** Madagascar
- ☒ **MK** The former Yugoslav Republic of Macedonia
- ☒ **MN** Mongolia
- ☒ **MW** Malawi
- ☒ **MX** Mexico
- ☒ **NO** Norway
- ☒ **NZ** New Zealand
- ☒ **PL** Poland
- ☒ **PT** Portugal
- ☒ **RO** Romania
- ☒ **RU** Russian Federation
- ☒ **SD** Sudan
- ☒ **SE** Sweden
- ☒ **SG** Singapore
- ☒ **SI** Slovenia
- ☒ **SK** Slovakia
- ☒ **SL** Sierra Leone
- ☒ **TJ** Tajikistan
- ☒ **TM** Turkmenistan
- ☒ **TR** Turkey
- ☒ **TT** Trinidad and Tobago
- ☒ **UA** Ukraine
- ☒ **UG** Uganda
- ☒ **US** United States of America
- ☒ **UZ** Uzbekistan
- ☒ **VN** Viet Nam
- ☒ **YU** Yugoslavia
- ☒ **ZW** Zimbabwe

Check-boxes reserved for designating States (for the purposes of a national patent) which have become party to the PCT after issuance of this sheet:

- ☒ GD. GRENADA
- ☐

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.)*

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplemental Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) 10 October 1997 (10-10-1997)	1007252	The Netherlands		
item (2)				
item (3)				

☒ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s): 1

** Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):* ISA /

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority):*
Date *(day/month/year)* Number Country *(or regional Office)*

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following **number of sheets**:

request	3
description (excluding sequence listing part)	9
claims	2
abstract	1
drawings	1
sequence listing part of description	
Total number of sheets	16

This international application is **accompanied by** the item(s) marked below:

1. ☒ fee calculation sheet
2. ☐ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☐ other *(specify)*:

Figure of the drawings which should accompany the abstract: Fig. 1

Language of filing of the international application: English

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

JORRITSMA, R.

Nederlandsch Octrooibureau, The Hague , October 9, 1998

For receiving Office use only

1. Date of actual receipt of the purported international application: 09 OCT 1998 (09.10.98)
2. Drawings: ☒ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:
4. Date of timely receipt of the required corrections under PCT Article 11(2):
5. International Searching Authority (if two or more are competent): ISA /
6. ☐ Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau: 10 NOVEMBER 1998 (10.11.98)

Werkwijze en inrichting voor het beveiligen van datacommunicatie

De uitvinding betreft een werkwijze en een inrichting voor het beveiligen van datacommunicatieverkeer tussen een eerste communicatiestation en een tweede communicatiestation, waarbij de data volgens een dataprotocol van het tweede naar het eerste communicatiestation wordt verstuurd. In het bijzonder worden datacommunicatieverbindingen beschermd, die middels openbare en/of private data- en telecommunicatie-infrastructuur benaderbaar zijn voor derden.

Op de markt bevinden zich in toenemende mate apparaten die zijn voorzien van een optie, die het mogelijk maakt om zogenaamde service op afstand te verlenen. Het gaat hier met name om opgestelde faxapparatuur, netwerk-faxapparatuur, telefoonmodems, kabelmodems, gecombineerde fax-modemconfiguraties, telefoontoestellen, antwoordapparaten, telefooncentrales, kopieermachines, wasmachines en andere huishoudelijke, industriële apparaten en bedrijfsapparaten, die via de genoemde infrastructuren met elkaar kunnen communiceren. Dit betreft apparaten die apart staan opgesteld, alsmede in combinatie met andere apparatuur. Deze service op afstand, ook bekend onder de engelse termen "remote diagnostics" of "remote maintenance" is ontwikkeld om op een flexibele en goedkope wijze ondersteuning te kunnen leveren aan de (eind)gebruikers van de apparatuur.

Service op afstand, verder aangeduid als RDS ("Remote DiagnosticS"), maakt het mogelijk om via de genoemde infrastructuur vanaf de lokatie van de leverancier of een ander servicepunt, het betreffende apparaat aan een analyse te onderwerpen. In een aantal gevallen is het zelfs mogelijk dat de servicemonteur op afstand kleine reparaties kan uitvoeren. Als blijkt dat reparatie toch op de lokatie van het apparaat uitgevoerd moet worden, kan de betreffende onderhoudsmonteur of -technicus met de juiste onderdelen op pad gestuurd worden. Via RDS is het namelijk reeds bekend wat er mankeert aan het apparaat en welke maatregelen genomen moeten worden om het euvel te verhelpen.

De functionaliteit van RDS kan vele geavanceerde opties omvatten:

- Het uitlezen van de diverse tellerstanden; door interpretatie van de tellerstanden kan bepaald worden wanneer een onderhoudsbeurt nodig is.

- Het in- en uitschakelen van de optische en akoestische signalen bij bv. een faxapparaat; hierdoor is het mogelijk het apparaat op afstand te analyseren zonder de directe omgeving te storen.
- Het uitlezen van een fax-/telefoonnummerlijst; bij een wijziging van (service) telefoonnummers kunnen deze op afstand gewijzigd worden.
- Het uitlezen van een faxjournaal; het journaal bevat meestal de foutencodes van de laatste verzonden faxberichten, welke door de technische ondersteuning gebruikt kunnen worden ten behoeve van de analyse van de apparatuur.
- Het manipuleren van het faxgeheugen; bedoeld om een laatste mogelijkheid te bieden voor het leegmaken van het geheugen als dit via de voorgeschreven manier niet mogelijk is.
- Het wijzigen van de configuratie-instellingen; als service kan het apparaat op afstand geconfigureerd worden volgens de wensen van de klant.
- Het toevoegen van doorschakelnummers; het servicecentrum kan dan zelf eventuele beschadigde faxen bekijken en daaruit afleiden wat de mogelijke oorzaak van de storing is.

Hoewel de genoemde functionaliteit is toegespitst op faxapparatuur kan een vergelijkbare functionaliteit aanwezig zijn in de andere hierboven genoemde apparatuur. De RDS-functionaliteit kan in principe alle functionaliteit bevatten, die bewerkingen met betrekking tot de in het apparaat aanwezige geheugens (RAM, ROM, EEPROM) betreffen.

Vele fabrikanten van datacommunicatie-inrichtingen maken gebruik van zogenaamde custom-chipsets (in grote aantallen geproduceerde standaard geïntegreerde schakelingen) of brengen in grote aantallen geproduceerde en aan vele fabrikanten geleverde hardware onder in een eigen-behuizing. De specificaties van de fabrikant zullen in vele gevallen alleen de door de fabrikant gewenste functies beschrijven. Het is dus mogelijk dat (RDS-)functionaliteit in custom-chipsets of hardware aanwezig is, die niet aan de eindgebruiker bekend wordt gemaakt.

In de huidige informatiemaatschappij is kennis macht. Informatie wordt natuurlijk goed beschermd, middels allerlei fysieke en organisatorische beveiligingsmaatregelen. Documenten mogen bijvoorbeeld alleen onder ogen komen van een selecte groep personen, waarna deze veilig in de kluis worden opgeborgen. Ten behoeve van een

snelle besluitvorming en verversing van de informatiepositie zal vaak telefonisch overleg worden gevoerd, waarbij veelvuldig van het fax-apparaat gebruik wordt gemaakt om de te bespreken documenten naar elkaar te verzenden. Hier ligt een zwak punt in de gehele beveiligingsketen. In wezen worden de betreffende documenten ter beschikking gesteld aan derden, waarvan het nu juist de bedoeling is dat dat wordt voorkomen. Deze derden, die misschien directe zakelijke belangen hebben of zich ophouden in de wereld van de informatiemakelaardij, kunnen de beschikking krijgen over waardevolle informatie. Dit kan zelfs zonder dat de eigenaar van die gevoelige informatie ook maar enige indicatie heeft, totdat het te laat is. De bedrijfsspion blijkt dan wel heel erg dichtbij te zijn en werkt nota bene samen met degene die zijn eigen informatie met alle middelen heeft beschermd.

Een fax-apparaat beschikt bijvoorbeeld, al dan niet bekend aan de eindgebruiker, over RDS-functionaliteit en kan daardoor door een derde worden gemanipuleerd. Deze derde kan er bijvoorbeeld voor zorgen dat het betreffende fax-apparaat reageert op bepaalde faxnummers en/of fax-identificatienummers. Bij het verzenden en/of ontvangen van faxen van/naar die faxnummers zal het faxapparaat bijvoorbeeld een extra exemplaar verzenden naar het door die derde opgegeven faxnummer. De gebruiker van het faxapparaat merkt hier echter niets van, omdat de optische en akoestische signalen kunnen worden uitgeschakeld, het zogenaamde fax-doorverbindingsnummer niet in de lijst met faxdoorverbindingsnummers hoeft voor te komen en ook het faxjournaal geen melding hoeft te maken van deze handeling. Desnoods wordt een kopie van de desbetreffende fax pas tijdens de nachtelijke uren, als niemand in het bedrijf aanwezig is, verzonden.

Bij een netwerk-fax of een modemfax, opgenomen in een netwerksysteem binnen een bedrijf, is het voor te stellen, dat een derde via deze fax of dit modem toegang verkrijgt tot het netwerksysteem. Hierdoor zou het mogelijk kunnen zijn op de hierboven vermelde wijze ook informatie te onttrekken aan het veilig veronderstelde netwerksysteem.

Doelstelling van de onderhavige uitvinding is een werkwijze en een inrichting te verschaffen voor het beveiligen van datacommunicatieverkeer, teneinde te voorkomen dat derden ongemerkt gebruik kunnen maken van in een communicatiestation aanwezige

functionaliteit.

De doelstelling wordt volgens de uitvinding bereikt middels een werkwijze van de bij aanhef gedefinieerde soort, gekenmerkt door de stappen van het vergelijken van het dataprotocol met tenminste één gestandaardiseerd protocol en het slechts doorvoeren van data waarvan het dataprotocol voldoet aan het tenminste ene gestandaardiseerde protocol, naar het eerste communicatiestation.

Herhalingen van commando's, of bepaalde combinaties van commando's, die ieder op zich tot het gestandaardiseerde protocol behoren, maar niet tot normaal, effectief datacommunicatieverkeer leiden, worden geacht niet tot het gestandaardiseerde protocol te behoren. Het is namelijk mogelijk dat dergelijke herhalingen of combinaties van commando's gebruikt worden om bepaalde RDS-functionaliteit in te schakelen.

Voordat, bijvoorbeeld bij een faxapparaat, kan worden overgegaan tot het ontvangen en/of verzenden van documenten, zullen de apparaten aan beide zijden van de communicatieverbinding elkaar moeten informeren over de status waarin zij verkeren. Na deze zogenaamde "hand-shake"-procedure wordt de informatie-uitwisseling op elkaar afgestemd. Beide apparaten zijn nu gereed en zullen de gewenste opdracht uitvoeren. Deze procedure en de informatie-uitwisseling, verloopt volgens internationaal vastgelegde standaarden, ook protocollen genoemd, die voor een deel zijn vastgelegd in de zogenaamde ISO-, ETSI- en ANSI-normen, of in voorschriften van de ITU. Voor, tijdens of na de "hand-shake"-procedure kan een controle plaatsvinden op de aanwezigheid van bepaalde RDS-functionaliteit. Voor het gebruik van RDS-functionaliteit zal een fabrikant protocollen gebruiken die niet (geheel) zijn opgenomen in de standaarden. Dit betekent dat het gebruik van een zogenaamd exotisch protocol kan duiden op het gebruik van RDS-functionaliteit. Het geeft in ieder geval aan dat de andere partij zich niet houdt aan de standaard protocollen. Het negeren van de standaard geeft een indicatie dat de gemaakte verbinding op een andere wijze wordt gebruikt dan de gebruiker bedoeld heeft.

Door het toepassen van de werkwijze volgens de uitvinding zal een poging van een derde om van buitenaf (verborgen) RDS-functionaliteit in te schakelen niet slagen, waardoor de kans dat informatie kan weglekken via de gebruikte communicatie-apparatuur

aanzienlijk kleiner wordt.

Omdat volgens de uitvinding het dataprotocol vergeleken wordt met gestandaardiseerde protocollen, is de werkwijze volgens de uitvinding wereldwijd toepasbaar.

In een uitvoeringsvorm van de werkwijze volgens de uitvinding wordt de gebruiker van een communicatiestation gewaarschuwd indien bij het vergelijken van het dataprotocol blijkt dat dit niet tot een bekend gestandaardiseerd protocol behoort. Hierdoor wordt de gebruiker gewaarschuwd van een poging van een derde om zijn communicatiestation te manipuleren, waarop de gebruiker direct actie kan ondernemen.

Een verdere uitvoeringsvorm van de werkwijze volgens de uitvinding wordt de verbinding onderbroken indien bij het vergelijken van het dataprotocol blijkt dat dit niet tot een gestandaardiseerd protocol behoort. Dit heeft als gevolg dat elke poging tot manipulatie van het communicatiestation door een derde niet zal slagen.

In een voorkeursuitvoeringsvorm van de werkwijze volgens de uitvinding wordt, na constatering dat het dataprotocol niet tot een bepaald gestandaardiseerd protocol behoort, een gegevensbestand met gegevens van het datacommunicatieverkeer en het tweede communicatiestation aangemaakt. Door deze gegevens vast te leggen, wordt de gebruiker in staat gesteld een zo volledig mogelijk beeld van de gebruiker van het tweede communicatiestation te verkrijgen, waarna passende maatregelen getroffen kunnen worden.

Een ander aspect van de uitvinding voorziet in een inrichting, geschikt om de werkwijze volgens de uitvinding uit te voeren. Hiertoe wordt de inrichting voorzien van geheugenmiddelen voor het opslaan van datakenmerken van een gestandaardiseerd protocol en vergelijk-/doorvoermiddelen voor het vergelijken van de opgeslagen datakenmerken met het dataprotocol en het slechts doorvoeren van data waarvan het dataprotocol voldoet aan het tenminste ene gestandaardiseerde protocol naar het eerste communicatiestation.

Met de inrichting volgens de uitvinding is het mogelijk de bovenvermelde werkwijze toe te passen in een datacommunicatie-omgeving. Voordeel van de inrichting volgens de uitvinding is dat de gebruiker onafhankelijk van het merk en type apparaat zelf kan bepalen of RDS-functionaliteit wordt toegelaten. Doordat de inrichting gescheiden van het lokale communicatiestation kan worden toegepast, hoeft bij aanschaf van het lokale communicatiestation niet te worden

gelet op eventuele aanwezige RDS-functionaliteit.

Door het geringe aantal benodigde onderdelen, is het mogelijk de inrichting compact, licht en robuust te vervaardigen, en aan te passen aan de situatie waarin deze toegepast wordt. Verder zijn de bediening en de aansluiting van de inrichting eenvoudig.

Bij voorkeur worden de geheugenmiddelen uitgevoerd als ROM-geheugen. Hierdoor is het niet mogelijk dat tijdens gebruik de inhoud van de geheugenmiddelen gemanipuleerd wordt, maar blijft het eenvoudig om middels het verwisselen van het ROM-geheugen de inrichting aan te passen aan de nieuwste gestandaardiseerde protocollen.

In een uitvoeringsvorm van de inrichting omvat de inrichting verder waarschuwingsmiddelen. Wanneer data gedetecteerd wordt, waarvan het dataprotocol niet voldoet aan het tenminste ene gestandaardiseerde protocol, wordt de gebruiker gewaarschuwd, bijvoorbeeld door visuele en/of akoestische waarschuwingsmiddelen. Hierdoor zal de gebruiker altijd gewaarschuwd worden als een poging tot manipulatie van het eerste communicatiestation wordt ondernomen, zelfs als daarbij wordt getracht indicaties van het eerste communicatiestation uit te schakelen.

Een verdere uitvoeringsvorm van de inrichting volgens de uitvinding omvat weergeefmiddelen, verbonden met de vergelijk-/doorvoermiddelen, waarbij de weergeefmiddelen gegevens omtrent het datacommunicatieverkeer en het tweede communicatiestation, welke opgeslagen zijn nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet voldoet aan het tenminste ene gestandaardiseerde protocol, weergeven. Dit kan bijvoorbeeld uitgevoerd worden als een weergeefscherm op de inrichting zelf.

Als aanvulling kan de inrichting in een verdere uitvoeringsvorm voorzien zijn van invoermiddelen, verbonden met de vergelijk-/doorvoermiddelen, voor het invoeren van commando's met betrekking tot het weergeven van de gegevens.

Een alternatieve uitvoeringsvorm van de uitvinding is om deze, in plaats van de weergeefmiddelen en/of de invoermiddelen, te voorzien van interfacemiddelen. Deze interfacemiddelen zorgen voor het uitwisselen van gegevens naar een externe verwerkingsinrichting betreffende het datacommunicatieverkeer en het tweede communicatiestation, welke gegevens opgeslagen zijn nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet voldoet aan

het tenminste ene gestandaardiseerde protocol. Deze verwerkingsinrichting kan bijvoorbeeld een computer zijn, waarmee de gegevens verder bewerkt en weergegeven kunnen worden.

Door middel van de weergave van deze gegevens wordt de gebruiker in staat gesteld een zo volledig mogelijk beeld van de poging tot manipulatie van het lokale communicatiestation te verkrijgen, waarna passende maatregelen getroffen kunnen worden.

Volgens een uitvoeringsvorm van de uitvinding kan de inrichting geïntegreerd worden met het lokale communicatiestation.

De werkwijze en de inrichting volgens de uitvinding zullen nu verder toegelicht worden aan de hand van de tekeningen.

Fig. 1 toont een schema van een uitvoeringsvorm volgens de uitvinding; en

Fig. 2 toont het stroomschema van de werkwijze volgens de uitvinding.

Fig. 1 toont een schema van een voorkeursuitvoeringsvorm volgens de uitvinding, waarbij de inrichting 10 voor het beveiligen van datacommunicatieverkeer verbonden is met een eerste communicatiestation 11 en een tweede communicatiestation 12. De inrichting 10 omvat vergelijk-/doorvoermiddelen 15, die tijdens bedrijf met zowel het eerste 11 als het tweede 12 communicatiestation kunnen communiceren. De inrichting 10 omvat verder geheugenmiddelen 14, verbonden met de vergelijk-/doorvoermiddelen 15. In de weergegeven voorkeursuitvoeringsvorm van de uitvinding omvat de inrichting 10 verder waarschuwingsmiddelen 16, weergeefmiddelen 17 en invoermiddelen 18, allen verbonden met de vergelijk-/doorvoermiddelen 15. De communicatiestations 11 en 12 kunnen bijvoorbeeld van een RDS-functionaliteit voorziene fax- of kopieerapparaten zijn.

In de geheugenmiddelen 14 zijn de kenmerken van datacommunicatie volgens tenminste één gestandaardiseerd protocol opgeslagen. De vergelijk-/doorvoermiddelen 15 dienen voor het vergelijken van het dataprotocol van data die het tweede communicatiestation 12 naar het eerste communicatiestation 11 wil sturen en het slechts doorvoeren van data waarvan het dataprotocol voldoet aan het tenminste ene gestandaardiseerde protocol, naar het lokale communicatiestation 11.

In de getoonde voorkeursuitvoeringsvorm omvat de inrichting 10 tevens waarschuwingsmiddelen 16, welke een waarschuwing geven nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet

voldoet aan het tenminste ene gestandaardiseerde protocol. In de figuur is aangegeven dat de waarschuwingsmiddelen 16 worden uitgevoerd als een waarschuwingslamp. Het is echter mogelijk om hiervoor andere visuele danwel akoestische waarschuwingsmiddelen te gebruiken.

Tevens omvat de inrichting 10 in de getoonde voorkeursuitvoeringsvorm van de uitvinding weergeefmiddelen 17 om gegevens omtrent het datacommunicatieverkeer en het tweede communicatiestation 12, die opgeslagen zijn nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet voldoet aan het tenminste ene gestandaardiseerde protocol, weer te geven. Verder omvat de inrichting invoermiddelen 18 voor het invoeren van commando's met betrekking tot het weergeven van de gegevens. Het is bijvoorbeeld mogelijk om commando's in te voeren om slechts een bepaald gedeelte van de gegevens weer te geven op de weergeefmiddelen.

In een niet getoonde uitvoeringsvorm van de uitvinding, omvat de inrichting 10 in plaats van de weergeefmiddelen 17 en invoermiddelen 18, interfacemiddelen, welke verbonden kunnen worden met een externe verwerkingsinrichting. Deze verwerkingsinrichting kan bijvoorbeeld een computer zijn, waarmee de gegevens verder bewerkt, opgeslagen en weergegeven kunnen worden.

In Fig. 2 wordt het stroomschema getoond van de werkwijze volgens de uitvinding. De werkwijze begint met het ontvangen van data van het tweede communicatiestation 12 in blok 1. In beslissingsblok 2 wordt het dataprotocol van de in blok 1 ontvangen data vergeleken met het gestandaardiseerde protocol. Indien het dataprotocol voldoet aan het tenminste ene gestandaardiseerde protocol, wordt de data doorgegeven naar het eerste communicatiestation 11 in doorgeefblok 3. Vervolgens gaat de werkwijze terug naar blok 1, voor het controleren van de verdere ontvangen data.

Indien het dataprotocol niet voldoet aan het tenminste ene gestandaardiseerde protocol, vervolgt de werkwijze de procedure in waarschuwingsblok 4, waarin de gebruiker gewaarschuwd wordt. De volgende stap in de procedure bestaat uit het onderbreekblok 6, waarin de verbinding met het tweede communicatiestation onderbroken wordt. Parallel aan waarschuwingsblok 4 en onderbreekblok 6 wordt in een voorkeursuitvoeringsvorm van de werkwijze volgens de uitvinding een gegevensbestand opgeslagen in blok 5, waarin gegevens van het datacommunicatieverkeer en het tweede communicatiestation opgeslagen

worden.

Met de in de figuren getoonde werkwijze en inrichting voor het beveiligen van datacommunicatieverkeer, zal een poging van een derde om van buitenaf (verborgen) functionaliteit in te schakelen niet slagen, waardoor de kans dat informatie kan weglekken via de gebruikte communicatie-apparatuur aanzienlijk kleiner wordt.

Door de gebruiker te waarschuwen en gegevens omtrent het datacommunicatieverkeer en het tweede communicatiestation 12 vast te leggen, wordt de gebruiker in staat gesteld een zo volledig mogelijk beeld van de gebruiker van het tweede communicatiestation te verkrijgen, waarna passende maatregelen getroffen kunnen worden.

Voordeel van de beschreven inrichting is dat de gebruiker onafhankelijk van het merk en type apparaat zelf kan bepalen of RDS-functionaliteit wordt toegelaten. Doordat de inrichting gescheiden van het eerste communicatiestation kan worden toegepast, hoeft bij aanschaf van het eerste communicatiestation niet te worden gelet op eventuele aanwezige RDS-functionaliteit. Uiteraard kan de inrichting 10 ook fysiek in het eerste communicatiestation 11 zijn opgenomen. De vergelijk-/doorvoermiddelen 15 kunnen in dat geval integraal onderdeel uitmaken van een in het eerste communicatiestation 11 aanwezige processor.

Door het vergelijken van het dataprotocol van de ontvangen data met gestandaardiseerde protocollen is de werkwijze volgens de uitvinding wereldwijd toepasbaar.

Door het geringe aantal benodigde onderdelen, is het mogelijk de inrichting compact, licht en robuust te vervaardigen, en aan te passen aan de situatie waarin deze toegepast wordt. Verder zijn de bediening en de aansluiting van de inrichting eenvoudig.

Indien de geheugenmiddelen uitgevoerd worden als ROM-geheugen, is het niet mogelijk dat tijdens gebruik de inhoud van de geheugenmiddelen 14 gemanipuleerd wordt, maar blijft het eenvoudig om middels het verwisselen van het ROM-geheugen de inrichting aan te passen aan de nieuwste gestandaardiseerde protocollen.

Hoewel de inrichting is beschreven voor het beveiligen van datacommunicatieverkeer tussen twee communicatiestations, is het natuurlijk ook mogelijk om het datacommunicatieverkeer tussen meerdere communicatiestations te beveiligen, zoals bijvoorbeeld in een netwerkomgeving.

Conclusies

1. Werkwijze voor het beveiligen van datacommunicatieverkeer tussen een eerste communicatiestation (11) en een tweede communicatiestation (12), waarbij de data volgens een dataprotocol van het tweede naar het eerste communicatiestation wordt verstuurd, gekenmerkt door de volgende stappen:

(i) het vergelijken van het dataprotocol met tenminste één gestandaardiseerd protocol;

(ii) het slechts doorvoeren van data waarvan het dataprotocol voldoet aan het tenminste ene gestandaardiseerde protocol, naar het eerste communicatiestation (11).

2. Werkwijze volgens conclusie 1, gekenmerkt doordat nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet voldoet aan het tenminste ene gestandaardiseerde protocol, een waarschuwing gegenereerd wordt.

3. Werkwijze volgens conclusie 1 of 2, gekenmerkt doordat nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet voldoet aan het tenminste ene gestandaardiseerde protocol, het datacommunicatieverkeer onderbroken wordt.

4. Werkwijze volgens een van de voorgaande conclusies, gekenmerkt doordat nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet voldoet aan het tenminste ene gestandaardiseerde protocol, een gegevensbestand met gegevens van het datacommunicatieverkeer en het tweede communicatiestation (12) opgeslagen wordt.

5. Inrichting voor het beveiligen van datacommunicatieverkeer tussen een eerste communicatiestation (11) en een tweede communicatiestation (12), waarbij data volgens een dataprotocol van het tweede naar het eerste communicatiestation wordt verstuurd, met het kenmerk dat de inrichting (10) omvat:

- geheugenmiddelen (14) waarin datakenmerken van tenminste één gestandaardiseerd protocol opgeslagen zijn;

- vergelijk-/doorvoermiddelen (15) voor het vergelijken van de opgeslagen datakenmerken met het dataprotocol en het slechts doorvoeren van data waarvan het dataprotocol voldoet aan het tenminste

ene gestandaardiseerde protocol, naar het eerste communicatiestation (11).

6. Inrichting volgens conclusie 5, met het kenmerk dat de inrichting verder waarschuwingsmiddelen (16) omvat, verbonden met de vergelijk-/doorvoermiddelen (15), welke een waarschuwing geven nadat bij het vergelijken van het dataprotocol gebleken is dat deze niet tot het tenminste ene gestandaardiseerde protocol behoort.

7. Inrichting volgens conclusie 5 of 6, met het kenmerk dat de inrichting verder weergeefmiddelen (17) omvat, verbonden met de vergelijk-/doorvoermiddelen (15), waarbij de weergeefmiddelen (17) gegevens omtrent het datacommunicatieverkeer en het tweede communicatiestation (12) weergeven, welke gegevens opgeslagen zijn nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet voldoet aan het tenminste ene gestandaardiseerde protocol.

8. Inrichting volgens conclusie 7, met het kenmerk dat de inrichting verder invoermiddelen (18) omvat, verbonden met de vergelijk-/doorvoermiddelen (15), voor het invoeren van commando's met betrekking tot het weergeven van de gegevens.

9. Inrichting volgens conclusie 5 of 6, met het kenmerk dat de inrichting interfacemiddelen omvat, voor het uitwisselen van gegevens omtrent het datacommunicatieverkeer en het tweede communicatiestation (12) met een externe verwerkingsinrichting, welke gegevens opgeslagen zijn nadat bij het vergelijken van het dataprotocol gebleken is dat dit niet voldoet aan het tenminste ene gestandaardiseerde protocol.

10. Inrichting volgens een van de conclusie 5 tot en met 9, met het kenmerk dat de inrichting (10) is geïntegreerd in het eerste communicatiestation (11).

****

PCT/NL 98 / 00081

Uittreksel

De uitvinding betreft een werkwijze en een inrichting voor het beveiligen van datacommunicatieverkeer tussen een eerste communicatiestation (11) en een tweede communicatiestation (12), waarbij de data volgens een dataprotocol van het tweede naar het eerste communicatiestation wordt verstuurd. De werkwijze omvat de stappen van het vergelijken van het dataprotocol met tenminste één gestandaardiseerd protocol en het slechts doorvoeren van data waarvan het dataprotocol voldoet aan het tenminste ene gestandaardiseerde protocol, naar het eerste communicatiestation (11).

De inrichting (10) omvat hiertoe geheugenmiddelen (14) waarin datakenmerken van tenminste één gestandaardiseerde protocol opgeslagen zijn en vergelijk-/doorvoermiddelen (15) welke de opgeslagen datakenmerken vergelijken met het dataprotocol en slechts data doorvoeren waarvan het dataprotocol voldoet aan het tenminste ene gestandaardiseerde protocol.

[Fig. 1]

Fig - 1

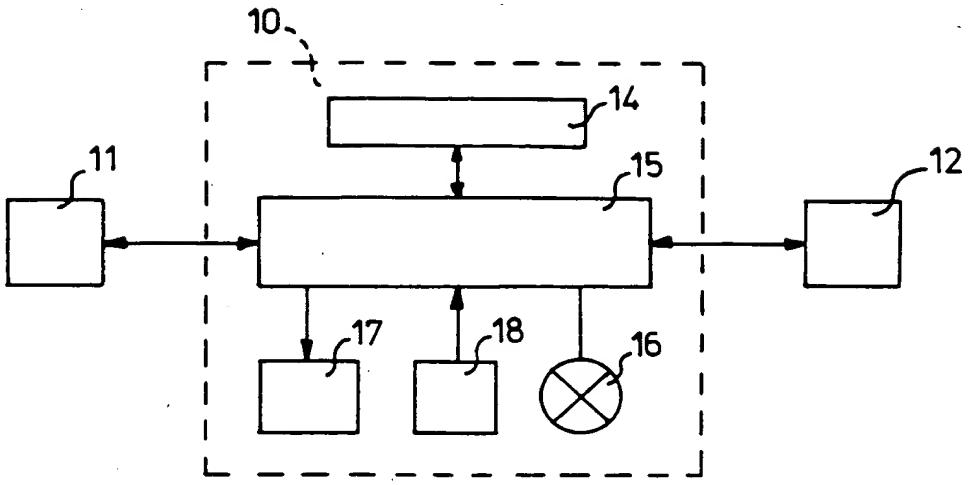

10
14
11
15
12
17
18
16

Fig - 2

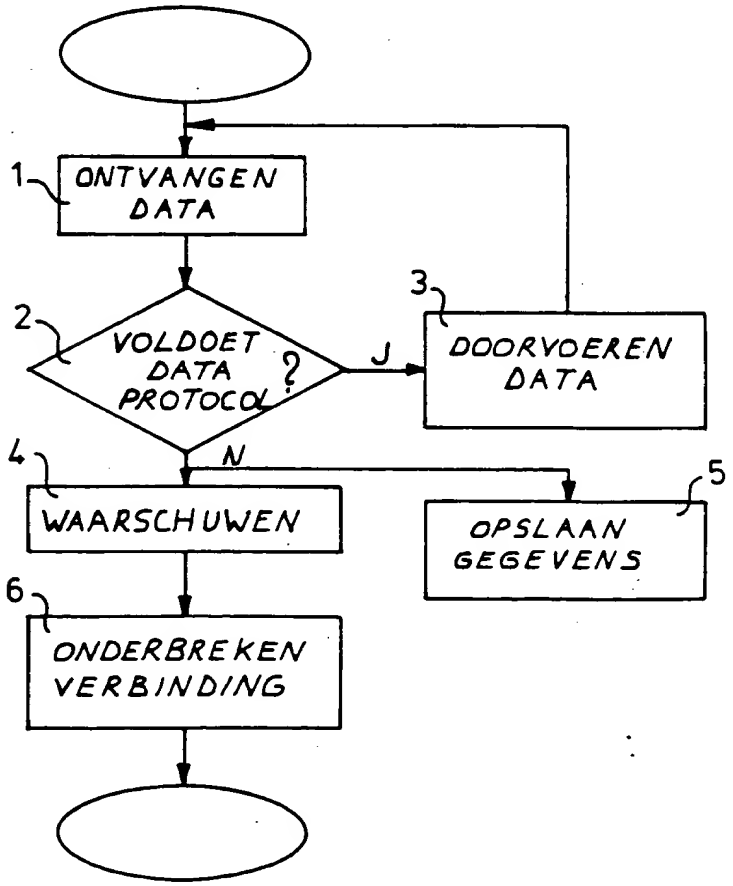

1
ONTVANGEN DATA
2
VOLDOET DATA PROTOCOL ?
J
3
DOORVOEREN DATA
N
4
WAARSCHUWEN
5
OPSLAAN GEGEVENS
6
ONDERBREKEN VERBINDING

Fig 1

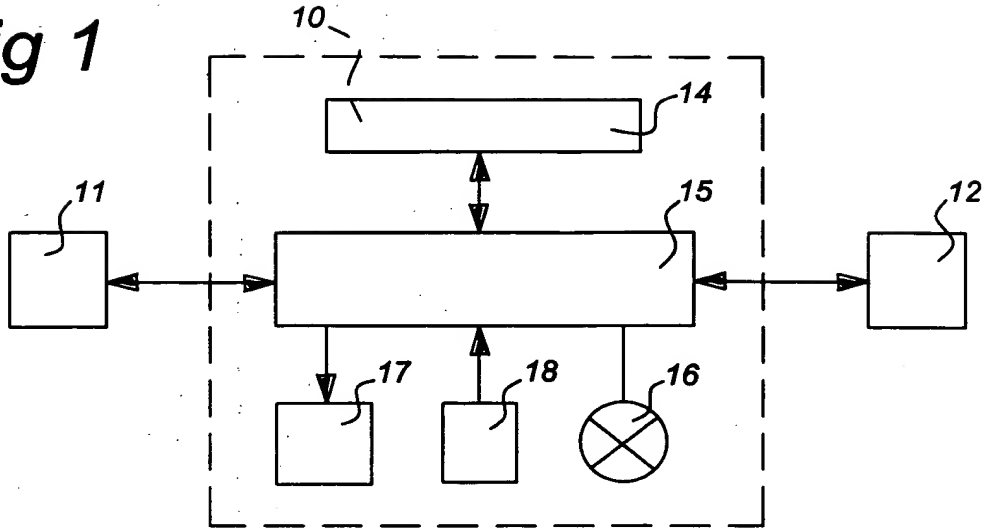
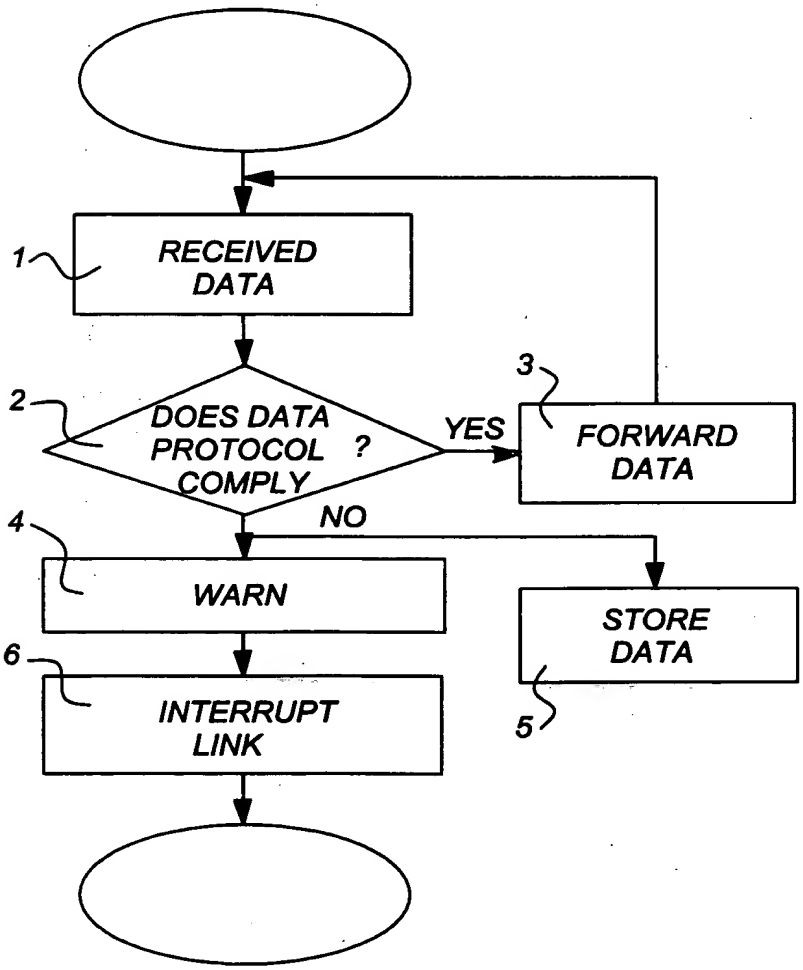

10
14
11
15
12
17
18
16

Fig 2


RECEIVED DATA
1
DOES DATA PROTOCOL COMPLY ?
2
YES
FORWARD DATA
3
NO
WARN
4
STORE DATA
5
INTERRUPT LINK
6

M.H

17

PATENT COOPERATION TREATY

PCT

REC'D 10 FEB 2000

WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
BO 41539 YK		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/NL98/00581	09/10/1998	10/10/1997

International Patent Classification (IPC) or national classification and IPC
H04L29/06

Applicant
DE LA BRETONIERE, Ralph, Rogier

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 9 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
07/05/1999	08.02.2000

Name and mailing address of the international preliminary examining authority:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized officer

Alonso, R

Telephone No. +49 89 2399 7515

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/NL98/00581

I. Basis of the r p rt

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

6-9	as originally filed			
1-5,5a	as received on	17/01/2000	with letter of	14/01/2000

Claims, No.:

1-9	as received on	17/01/2000	with letter of	14/01/2000

Drawings, sheets:

1/1	as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with r gard to nov lty, inv ntiv step r industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims 1-9
	No:	Claims
Inventive step (IS)	Yes:	Claims 1-9
	No:	Claims
Industrial applicability (IA)	Yes:	Claims 1-9
	No:	Claims

2. Citations and explanations

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

V. Reasoned statement under Article 35 (2) (N, IS, IA)

The following document has been considered for the purposes of this report:

D1= US-A-5124984

*****

The present application relates to a method (claim 1) and a device (independent claim 4) for protecting data communication traffic through a communication link.

Document D1 (considered as the closest prior art) describes an access controller for communication networks which monitors the data packets transmitted between stations, determines when an improper type of access is being made and either destroys the packet or transmits one or more packets which cause the termination or alteration of the communication between two stations.

The problem with the prior art is that some packets might reach the receiving station before the termination mechanism can end the data communication.

The solution of the invention, as set out in the two independent claims, is a data protection method and a device wherein data sent from a first station to a second station pass through the device, said device forwarding the data to the second station only if the data complies with a standardised protocol.

This principle is neither disclosed nor rendered obvious by the available prior art. The subject-matter of independent claims 1 and 4, and dependent claims 2, 3 and 5 to 9 involves an inventive step and the mentioned claims are therefore considered to meet the requirements of Article 33 PCT with regard to novelty, inventive step and industrial applicability.

VIII. Certain observations on the international application

Independent claim 8 does not meet the requirements of Article 6 PCT for the reasons set out below:

The expression 'providing the data communication protection device in the communication link' is unclear. It appears to be meant that the protection device is part of the physical path between the communication stations and, in that sense, a clearer expression should have been used.

Method and device for protecting data communication

The invention relates to a method and a device for protecting data communication traffic through a communication link between a first communication station and a second communication station, in which the data is dispatched according to a data protocol from the second communication station to the first communication station, comprising the steps of (i) receiving the data from the second communication station in a data communication protection device and (ii) comparing the data protocol of the data with at least one standardised protocol in the data communication protection device. In particular, data communication links are protected which can be seized by third parties by means of public and/or private data and telecommunication infrastructure.

Furthermore, the present invention relates to a data communication protection device arranged for protecting data communication traffic between a first communication station and a second communication station, data being dispatched according to a data protocol from the second communication station to the first communication station, the data communication protection device comprising memory means for storing data characteristics of at least one standardised protocol, the data communication protection device further being arranged for comparing the data protocol of the data with the at least one standardised protocol.

Such a method and device are known from US-A-5,124,984, which discloses a method for protecting data communication traffic between a first communication station and a second communication station, in which the data is dispatched according to a data protocol from the second to the first communication station, in which the data protocol is compared with at least one standardised protocol and data is forwarded to the first communication station only when the data protocol complies with the at least one standardised protocol. The disclosed method and system are directed to data networks, the network interconnecting a number of stations and a network access controller. The network access controller is connected to the network and listens in on the data traffic on the network. The network access controller checks the content of each data package sent on the network and determines whether the packet is of an authorised type. It relies on control mechanisms present in the protocol that is being used in order to terminate communications between specific stations. It is disclosed that the network access controller 16 is not part of the physical path between communication stations.

Appliances are found to an increasing extent on the market which are provided with an option which makes it possible to provide so-called remote service. This involves, in particular, installed fax equipment, network fax equipment, telephone modems, cable modems, combined fax/modem configurations, telephone sets, answering machines,

telephone exchanges, copying machines, washing machines and other domestic, industrial appliances and operating appliances which can communicate with one another via the said infrastructures. This relates to appliances which are installed separately and also in combination with other equipment. This remote service, also known as "remote diagnostics" or "remote maintenance" has been developed in order to be able to deliver a flexible and cheap method of support to the (end) users of the equipment.

Remote service, furthermore referred to as RDS ("Remote DiagnosticS") makes it possible to subject the respective appliance to an analysis via the said infrastructure from the location of the supplier or another service point. In a number of cases, it is even possible for the service engineer to be able to carry out small repairs remotely. If it emerges that repair has nevertheless to be carried out at the location of the appliance, the respective maintenance engineer or technician can be sent out with the correct components. Specifically, it is already known via RDS what is wrong with the appliance and what measures have to be taken to remedy the fault.

The functionality of RDS may comprise many advanced options:

- The reading-out of the various counter positions; when a service is necessary can be determined by interpreting the counter positions.
- The switching-on and switching-off of the visual and audible signals, for example, in the case of a fax machine; as a result it is possible to analyse the appliance remotely without disturbing the immediate environment.
- The reading-out of a fax/telephone number list; in the event of an alteration of (service) telephone numbers, these can be altered remotely.
- The reading-out of a fax log; the log usually contains the error codes of the last fax messages sent and these can be used by the technical support for the purpose of analysing the appliance.
- The manipulation of the fax memory; this is intended to offer a final possibility for erasing the memory if this is not possible by means of the prescribed manner.
- The alteration of the configuration settings; as a service, the appliance can be configured remotely in accordance with the wishes of the client.
- The adding of connecting-through numbers; the service centre can then examine any damaged faxes itself and infer therefrom what the possible cause of the fault is.

Although the functionality mentioned is concentrated on fax machines, a comparable functionality may be present in the other equipment mentioned above. The RDS functionality can, in principle, comprise all the functionality which relates to operations concerning the memories (RAM, ROM, EEPROM) present in the appliance.

Many manufacturers of data communication devices make use of so-called custom chip sets (standard integrated circuits produced in large numbers) or accommodate hardware produced in large numbers and delivered to many manufacturers in a separate housing. The specifications of the manufacturer will, in many cases, describe only the functions desired by the manufacturer. It is therefore possible that (RDS) functionality is present in custom chip sets or hardware which is not made known to the end user.

In the modern information society, knowledge is power. Information is, of course, well protected by means of physical and organizational protection measures of all kinds. Documents may, for example, be seen only by a select group of individuals, after which they are securely stored in the safe. For the purpose of rapid decision-making and refreshing the information situation, consultation will often be made by telephone, in which case use is frequently made of the fax machine to transmit the documents to be discussed to one another. It is here that there is a weak point in the entire security chain. Essentially, the respective documents are made available to third parties, the intention being precisely to avoid that. Said third parties, who possibly have direct business interests or operate in the world of information brokerage, may acquire possession of valuable information. This may take place even without the owner of the sensitive information even having any indication until it is too late. The industrial spy therefore appears to be very near at hand and works, it is to be noted, together with the individual who has protected his own information with every means.

A fax machine has, for example, RDS functionality, whether this is known to the end user or not, and can thereby be manipulated by a third party. Said third party can ensure, for example, that the respective fax machine responds to certain fax numbers and/or fax identification numbers. During the transmission and/or reception of faxes from/to these fax numbers, the fax machine will transmit, for example, an additional copy to the fax number specified by said third party. The user of the fax machine does not, however, notice anything in this case because the visual and audible signals can be switched off, the so-called fax through-connection number does not have to figure in the list of fax through-connection numbers and even the fax log does not have to report this

operation. If necessary, a copy of the fax involved is transmitted only during the night hours when no-one is present in the company.

In the case of a network fax or a modem fax incorporated in a network system within a company, it is conceivable that a third party obtains access via said fax or said modem to the network system. As a result, it might be possible also to extract information in the manner mentioned above from the network system, which is believed to be safe.

The object of the present invention is to provide a method and a device for protecting data communication traffic in order to prevent third parties being able to make unnoticed use of functionality present in a communication station.

According to the invention, the object is achieved by means of a method of the type defined in the introduction, characterized by the steps of (iii) providing the data communication protection device in the communication link, the data from the second communication station to the first communication station passing through the data communication protection device and (iv) forwarding data of which the data protocol complies with the at least one standardised protocol from the data communication protection device to the first communication station, and not forwarding data of which the data protocol does not comply with the at least one standardised protocol from the data communication protection device to the first communication station.

Repetitions of commands, or certain combinations of commands, which each belong per se to the standardized protocol but do not lead to normal, effective data communication traffic, are deemed not to belong to the standardized protocol. Specifically, it is possible that such repetitions or combinations of commands are used to switch on certain RDS functionality.

Before a fax machine, for example, can proceed to the reception and/or transmission of documents, the appliances at both ends of the communication link have to inform one another about the status they are in. After this so-called "handshake" procedure, the information exchange is mutually adapted. Both appliances are now ready and will carry out the desired task. This procedure and the information exchange proceeds according to internationally specified standards, also referred to as protocols, which are specified in part in the so-called ISO, ETSI and ANSI standards or in the ITU regulations. Before, during or after the "handshake" procedure, a check can take place on the presence of certain RDS functionality. To use RDS functionality, a manufacturer will use protocols which are not (entirely) incorporated in the standards. This means that the use of a so-called exotic protocol can indicate the use of RDS functionality. It indicates in any case

that the other party is not adhering to the standard protocols. The negation of the standard indicates that the link made is being used in a manner other than that which the user intended.

As a result of using the method according to the invention, an attempt of a third party to switch on (concealed) RDS functionality from the outside will be unsuccessful, as a result of which the probability that information can leak out via the communication equipment used becomes substantially smaller.

Because, according to the invention, the data protocol is compared with standardized protocols, the method according to the invention can be used worldwide.

In an embodiment of the method according to the invention, the user of a communication station is warned if it emerges during the comparison of the data protocol that the latter does not belong to a known standardized protocol. As a result, the user is warned of an attempt of a third party to manipulate his communication station, whereupon the user can take direct action.

In a further embodiment of the method according to the invention, the link is interrupted if it emerges during the comparison of the data protocol that the latter does not belong to a standardized protocol. This has the result that any attempt to manipulate the communication station by a third party will be unsuccessful.

In a preferred embodiment of the method according to the invention, after ascertaining that the data protocol does not belong to a certain standardized protocol, a data file containing data of the data communication traffic and the second communication station is prepared. As a result of recording said data, the user is enabled to obtain as complete a picture as possible of the user of the second communication station, after which appropriate measures can be taken.

Another aspect of the invention provides a device suitable for carrying out the method according to the invention as defined in the preamble of claim 4. For this purpose, the device is further provided with a first link for linking the data communication protection device to the first communication station, and a second link for linking the data communication protection device to the second communication station, the data passing from the second communication station to the first communication station through the data communication protection device and comparison/forwarding means for forwarding data received through the second link of which the data protocol complies with the at least one standardised protocol from the data communication protection device through the first link, and not forwarding data of which the

data protocol does not comply with the at least one standardised protocol from the data communication protection device through the first link.

With the device according to the invention, it is possible to use the abovementioned method in a data communication environment. An advantage of the device according to the invention is that the user can determine himself, regardless of the brand and type of appliance, whether RDS functionality is permitted. Because the device can be used separately from the local communication station, there is no need to pay attention to any RDS functionality present when purchasing the local communication station.

As a result of the small number of components required, it is possible to manufacture the device in a compact, lightweight and robust form and to adapt it to the situation in which it is used. Furthermore, the operation and the connection of the device are simple.

Preferably, the memory means are designed as a ROM memory. As a result, it is impossible for the contents of the memory means to be manipulated during use, but it is still simple to adapt the device to the latest standardized protocols by replacing the ROM memory.

In an embodiment of the device, the device furthermore comprises warning means. If data is detected of which the data protocol does not comply with the at least one standardized protocol, the user is warned, for example by visual and/or audible warning means. As a result, the user will always be warned if an attempt is made to manipulate the first communication station, even if an attempt is made in these circumstances to switch off indications of the first communication station.

A further embodiment of the device according to the invention comprises display means linked to the comparison/forwarding means, the

CLAIMS

1. Method for protecting data communication traffic through a communication link between a first communication station (11) and a second communication station (12), in which the data is dispatched according to a data protocol from the second communication station to the first communication station, comprising the steps of:

(i) receiving the data from the second communication station (12) in a data communication protection device (10);

(ii) comparing the data protocol of the data with at least one standardised protocol in the data communication protection device (10), characterised by

(iii) providing the data communication protection device (10) in the communication link, the data from the second communication station (12) to the first communication station (11) passing through the data communication protection device (10); and

(iv) forwarding data of which the data protocol complies with the at least one standardised protocol from the data communication protection device (10) to the first communication station (11), and not forwarding data of which the data protocol does not comply with the at least one standardised protocol from the data communication protection device to the first communication station.

2. Method according to Claim 1, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a warning is generated.

3. Method according to one of the preceding claims, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a data file containing data of the data communication traffic and the second communication station (12) is stored.

4. Data communication protection device (10) arranged for protecting data communication traffic between a first communication station (11) and a second communication station (12), data being dispatched according to a data protocol from the second communication station to the first communication station, the data communication protection device comprising memory means (14) for storing data characteristics of at least one standardised protocol, the data communication protection device (10) further being

arranged for comparing the data protocol of the data with the at least one standardised protocol, characterised in that the data communication protection device (10) further comprises

- a first link for linking the data communication protection device (10) to the first communication station (11), and a second link for linking the data communication protection device (10) to the second communication station (12), the data passing from the second communication station to the first communication station through the data communication protection device;

- comparison/forwarding means (15) for forwarding data received through the second link of which the data protocol complies with the at least one standardised protocol from the data communication protection device (10) through the first link, and not forwarding data of which the data protocol does not comply with the at least one standardised protocol from the data communication protection device (10) through the first link.

5. Data communication device according to Claim 4, characterized in that the device furthermore comprises warning means (16) linked to the comparison/forwarding means (15) which give a warning after it has emerged during the comparison of the data protocol that it does not belong to the at least one standardized protocol.

6. Device according to Claim 4 or 5, characterized in that the device furthermore comprises display means (17) linked to the comparison/forwarding means (15), the display means (17) displaying data relating to the data communication traffic and the second communication station (12), which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

7. Device according to Claim 6, characterized in that the device furthermore comprises input means (18) linked to the comparison/forwarding means (15) for inputting commands relating to the display of the data.

8. Device according to Claim 4 or 5, characterized in that the device comprises interface means for exchanging data relating to the data communication traffic and the

second communication station (12) with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

9. Device according to one of Claims 4 to 8, characterized in that the device (10) is integrated in the first communication station (11).

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 29/06, G03G 15/00, H04N 1/32 — A1

(11) International Publication Number: **WO 99/20024**

(43) International Publication Date: 22 April 1999 (22.04.99)

(21) International Application Number: PCT/NL98/00581

(22) International Filing Date: 9 October 1998 (09.10.98)

(30) Priority Data:
1007252 10 October 1997 (10.10.97) NL

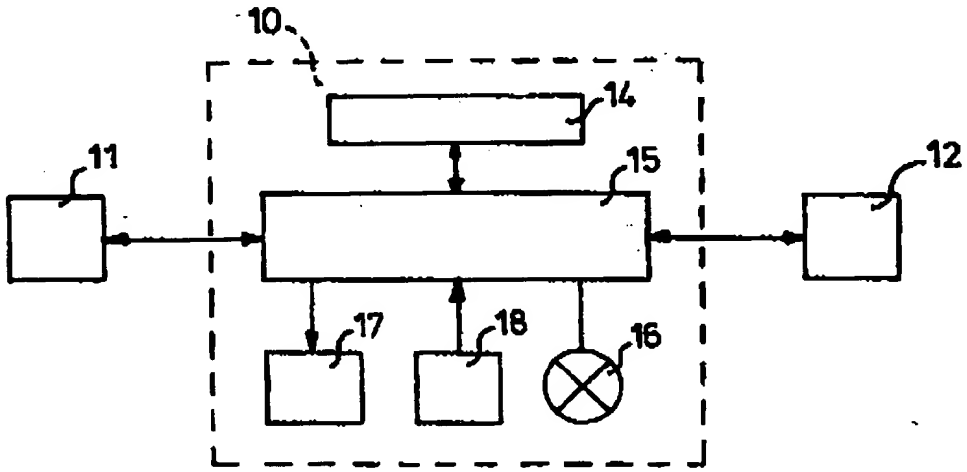
(71)(72) Applicant and Inventor: DE LA BRETONIERE, Ralph, Rogier [NL/NL]; Bijhouwerlommer 43, NL-2728 JK Zoetermeer (NL).

(74) Agent: DE BRUIJN, Leendert, C.; Nederlandsch Octrooibureau, Scheveningseweg 82, P.O. Box 29720, NL-2502 LS The Hague (NL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Dutch).

(54) Title: METHOD AND DEVICE FOR PROTECTING DATA COMMUNICATION



(57) Abstract

The invention relates to a method and a device for protecting data communication traffic between a first communication station (11) and a second communication station (12), in which the data is dispatched according to a data protocol from the second to the first communicati n station. The method comprises the steps of the comparison of the data protocol with at least one standardized protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station (11). For this purpose, the device (10) comprises memory means (14) in which data characteristics of at least one standardized protocol have been stored and comparison/forwarding means (15) which compare the stored data characteristics with the data protocol and forward only data of which the data protocol complies with the at least one standardized protocol.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

WO 99/20024 PCT/NL98/00581

Method and device for protecting data communication

The invention relates to a method and a device for protecting data communication traffic between a first communication station and a second communication station, in which the data is dispatched according to a data protocol from the second to the first communication station. In particular, data communication links are protected which can be seized by third parties by means of public and/or private data and telecommunication infrastructure.

Appliances are found to an increasing extent on the market which are provided with an option which makes it possible to provide so-called remote service. This involves, in particular, installed fax equipment, network fax equipment, telephone modems, cable modems, combined fax/modem configurations, telephone sets, answering machines, telephone exchanges, copying machines, washing machines and other domestic, industrial appliances and operating appliances which can communicate with one another via the said infrastructures. This relates to appliances which are installed separately and also in combination with other equipment. This remote service, also known as "remote diagnostics" or "remote maintenance" has been developed in order to be able to deliver a flexible and cheap method of support to the (end) users of the equipment.

Remote service, furthermore referred to as RDS ("Remote DiagnosticS") makes it possible to subject the respective appliance to an analysis via the said infrastructure from the location of the supplier r another service point. In a number of cases, it is even possible for the service engineer to be able to carry out small repairs remotely. If it emerges that repair has nevertheless to be carried out at the location of the appliance, the respective maintenance engineer or technician can be sent out with the correct components. Specifically, it is already known via RDS what is wrong with the appliance and what measures have to be taken to remedy the fault.

The functionality of RDS may comprise many advanced options:

- The reading-out of the various counter positions; when a service is necessary can be determined by interpreting the counter positions.
- The switching-on and switching-off of the visual and audible signals, for example, in the case of a fax machine; as a result it is possible to analyse the appliance remotely without disturbing the immediate environment.

- The reading-out of a fax/telephone number list; in the event of an alteration of (service) t lephone numbers, these can be altered remotely.
- The reading-out of a fax log; the log usually contains the error codes of the last fax messages sent and these can be used by the technical support for the purpose of analysing the appliance.
- The manipulation of the fax memory; this is intended to offer a final possibility for erasing the memory if this is not possible by means of the prescribed manner.
- The alteration of the configuration settings; as a service, the appliance can be configured remotely in accordance with the wishes of the client.
- The adding of connecting-through numbers; the service centre can then examine any damaged faxes itself and infer therefrom what the possible cause of the fault is.

Although the functionality mentioned is concentrated on fax machines, a comparable functionality may be present in the other equipment mentioned above. The RDS functionality can, in principle, comprise all the functionality which relates to operations concerning the memories (RAM, ROM, EEPROM) present in the appliance.

Many manufacturers of data communication devices make use of so-called custom chip sets (standard integrated circuits produced in large numbers) or accommodate hardware produced in large numbers and delivered to many manufacturers in a separate housing. The specifications of the manufacturer will, in many cases, describe only the functions desired by the manufacturer. It is therefore possible that (RDS) functionality is present in custom chip sets or hardware which is not made known to the end user.

In the modern information society, knowledge is power. Information is, of course, well protected by means of physical and organizational protection measures of all kinds. Documents may, for example, be seen only by a select group of individuals, after which they are securely stored in the safe. For the purpose of rapid decision-making and refreshing the information situation, consultation will often be made by telephone, in which case use is frequently made of the fax machine to transmit the documents to be discussed to one another. It is here that there is a weak point in the entire security chain. Essentially, the resp ctive documents are made available to third parties, the intention

being precisely to avoid that. Said third parties, who possibly have direct business interests or operate in the world of information brokerage, may acquire possession of valuabl information. This may take place even without the owner of the sensitive information even having any indication until it is too late. The industrial spy therefore appears to be very near at hand and works, it is to be noted, together with the individual who has protected his own information with every means.

A fax machine has, for example, RDS functionality, whether this is known to the end user or not, and can thereby be manipulated by a third party. Said third party can ensure, for example, that the respective fax machine responds to certain fax numbers and/or fax identification numbers. During the transmission and/or reception of faxes from/to these fax numbers, the fax machine will transmit, for example, an additional copy to the fax number specified by said third party. The user of the fax machine does not, however, notice anything in this case because the visual and audible signals can be switched off, the so-called fax through-connection number does not have to figure in the list of fax through-connection numbers and even the fax log does not have to report this operation, If necessary, a copy of the fax involved is transmitted only during the night hours when no-one is present in the company.

In the case of a network fax or a modem fax incorporated in a network system within a company, it is conceivable that a third party obtains access via said fax or said modem to the network system. As a result, it might be possible also to extract information in the manner mentioned above from the network system, which is believed to be safe.

The object of the present invention is to provide a method and a device for protecting data communication traffic in order to prevent third parties being able to make unnoticed use of functionality present in a communication station.

According to the invention, the object is achieved by means of a method of the type defined in the introduction, characterized by the steps of the comparison of the data protocol with at least one standardized protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station.

Repetitions of commands, or certain combinations of commands, which each belong per se to the standardized protocol but do not lead to normal, effective data communication traffic, are deemed not to belong to the standardized protocol. Specifically, it is possible that such

repetitions or combinations of commands are used to switch on certain RDS functionality.

Before a fax machine, for example, can proceed t the reception and/or transmission of documents, the appliances at both ends of the communication link have to inform one another about the status they are in. After this so-called "handshake" procedure, the information exchange is mutually adapted. Both appliances are now ready and will carry out the desired task. This procedure and the information exchange proceeds according to internationally specified standards, also referred to as protocols, which are specified in part in the so-called ISO, ETSI and ANSI standards or in the ITU regulations. Before, during or after the "handshake" procedure, a check can take place on the presence of certain RDS functionality. To use RDS functionality, a manufacturer will use protocols which are not (entirely) incorporated in the standards. This means that the use of a so-called exotic protocol can indicate the use of RDS functionality. It indicates in any case that the other party is not adhering to the standard protocols. The negation of the standard indicates that the link made is being used in a manner other than that which the user intended.

As a result of using the method according to the invention, an attempt of a third party to switch on (concealed) RDS functionality from the outside will be unsuccessful, as a result of which the probability that information can leak out via the communication equipment used becomes substantially smaller.

Because, according to the invention, the data protocol is compared with standardized protocols, the method according to the invention can be used worldwide.

In an embodiment of the method according to the invention, the user of a communication station is warned if it emerges during the comparison of the data protocol that the latter does not belong to a known standardized protocol. As a result, the user is warned of an attempt of a third party to manipulate his communication station, whereupon the user can take direct action.

In a further embodiment of the method according to the inv ntion, the link is interrupted if it emerges during the comparison of the data protocol that the latter does not belong to a standardized protocol. This has th result that any attempt to manipulate the communication station by a third party will be unsuccessful.

In a preferred embodiment of the method according to the

invention, after ascertaining that the data protocol does not belong to a certain standardized protocol, a data file c ntaining data of the data communication traffic and the second communication station is prepared. As a result of recording said data, the user is enabled to obtain as complete a picture as possible of the user of the second communication station, after which appropriate measures can be taken.

Another aspect of the invention provides a device suitable for carrying out the method according to the invention. For this purpose, the device is provided with memory means for storing data characteristics of a standardized protocol and comparison/forwarding means for the comparison of the stored data characteristics with the data protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station.

With the device according to the invention, it is possible to use the abovementioned method in a data communication environment. An advantage of the device according to the invention is that the user can determine himself, regardless of the brand and type of appliance, whether RDS functionality is permitted. Because the device can be used separately from the local communication station, there is no need to pay attention to any RDS functionality present when purchasing the local communication station.

As a result of the small number of components required, it is possible to manufacture the device in a compact, lightweight and robust form and to adapt it to the situation in which it is used. Furthermore, the operation and the connection of the device are simple.

Preferably, the memory means are designed as a ROM memory. As a result, it is impossible for the contents of the memory means to be manipulated during use, but it is still simple to adapt the device to the latest standardized protocols by replacing the ROM memory.

In an embodiment of the device, the device furthermore comprises warning means. If data is detected of which the data protocol does not comply with the at least one standardized protocol, the user is warned, for example by visual and/or audible warning means. As a result, the user will always be warned if an attempt is made to manipulate the first communication station, even if an attempt is made in th se circumstances to switch off indications of the first communication station.

A further embodiment of the device according to the invention comprises display means linked to the comparison/forwarding means, the

CLAIMS

1. Method for protecting data communication traffic between a first communication station (11) and a second communication station (12), in which the data is dispatched according to a data protocol from the second to the first communication station, characterized by the following steps:

(i) the comparison of the data protocol with at least one standardized protocol;

(ii) the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station (11).

2. Method according to Claim 1, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a warning is generated.

3. Method according to Claim 1 or 2, characterized in that, aft r it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, the data communication traffic is interrupted.

4. Method according to one of the preceding claims, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a data file containing data of the data communication traffic and the second communication station (12) is stored.

5. Device for protecting data communication traffic between a first communication station (11) and a second communication station (12), data being dispatched according to a data protocol from the second to the first communication station, characterized in that the device (10) comprises:

- memory means (14) in which data characteristics of at least one standardized protocol are stored;

- comparison/forwarding means (15) for the comparison of the stored data characteristics with the data protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station (11).

6. Device according to Claim 5, characterized in that the device furthermore comprises warning means (16) linked to the comparison/forwarding means (15) which give a warning after it has emerged during the comparison of the data protocol that it does not

belong to the at least one standardized protocol.

7. Device according to Claim 5 or 6, characterized in that th device furthermore comprises display means (17) linked to the comparison/forwarding means (15), the display means (17) displaying data relating to the data communication traffic and the second communication station (12), which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

8. Device according to Claim 7, characterized in that the device furthermore comprises input means (18) linked to the comparison/forwarding means (15) for inputting commands relating to the display of the data.

9. Device according to Claim 5 or 6, characterized in that the device comprises interface means for exchanging data relating to the data communication traffic and the second communication station (12) with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

10. Device according to one of Claims 5 to 9, characterized in that the device (10) is integrated in the first communication station (11).

09/509983

PCT/NL98/00581

WO 99/20024

Fig 1

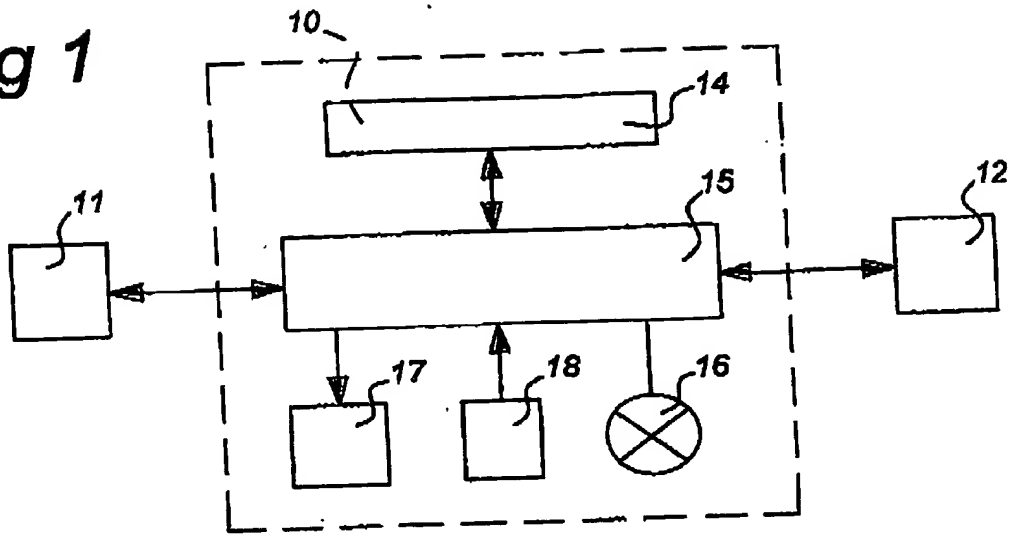
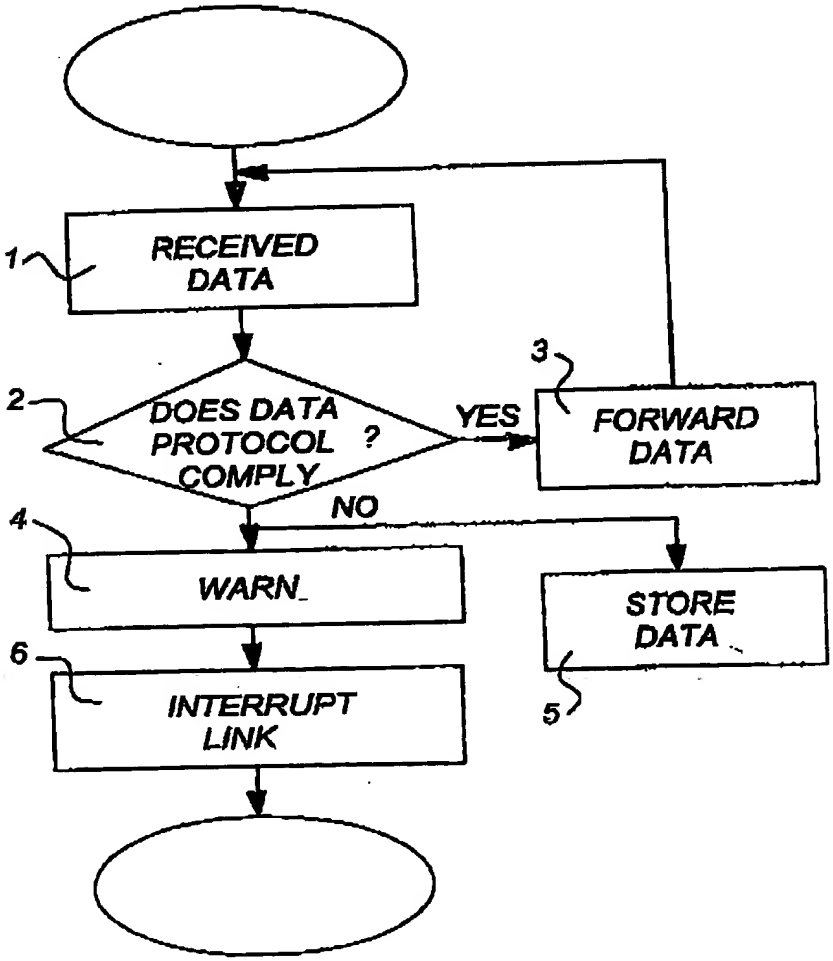


Fig 2



Method and device for protecting data communication

The invention relates to a method and a device for protecting data communication traffic between a first communication station and a second communication station, in which the data is dispatched according to a data protocol from the second to the first communication station. In particular, data communication links are protected which can be seized by third parties by means of public and/or private data and telecommunication infrastructure.

Appliances are found to an increasing extent on the market which are provided with an option which makes it possible to provide so-called remote service. This involves, in particular, installed fax equipment, network fax equipment, telephone modems, cable modems, combined fax/modem configurations, telephone sets, answering machines, telephone exchanges, copying machines, washing machines and other domestic, industrial appliances and operating appliances which can communicate with one another via the said infrastructures. This relates to appliances which are installed separately and also in combination with other equipment. This remote service, also known as "remote diagnostics" or "remote maintenance" has been developed in order to be able to deliver a flexible and cheap method of support to the (end) users of the equipment.

Remote service, furthermore referred to as RDS ("Remote DiagnosticS") makes it possible to subject the respective appliance to an analysis via the said infrastructure from the location of the supplier or another service point. In a number of cases, it is even possible for the service engineer to be able to carry out small repairs remotely. If it emerges that repair has nevertheless to be carried out at the location of the appliance, the respective maintenance engineer or technician can be sent out with the correct components. Specifically, it is already known via RDS what is wrong with the appliance and what measures have to be taken to remedy the fault.

The functionality of RDS may comprise many advanced options:

- The reading-out of the various counter positions; when a service is necessary can be determined by interpreting the counter positions.
- The switching-on and switching-off of the visual and audible signals, for example, in the case of a fax machine; as a result it is possible to analyse the appliance remotely without disturbing the immediate environment.

- The reading-out of a fax/telephone number list; in the event of an alteration of (service) telephone numbers, these can be altered remotely.
- The reading-out of a fax log; the log usually contains the error codes of the last fax messages sent and these can be used by the technical support for the purpose of analysing the appliance.
- The manipulation of the fax memory; this is intended to offer a final possibility for erasing the memory if this is not possible by means of the prescribed manner.
- The alteration of the configuration settings; as a service, the appliance can be configured remotely in accordance with the wishes of the client.
- The adding of connecting-through numbers; the service centre can then examine any damaged faxes itself and infer therefrom what the possible cause of the fault is.

Although the functionality mentioned is concentrated on fax machines, a comparable functionality may be present in the other equipment mentioned above. The RDS functionality can, in principle, comprise all the functionality which relates to operations concerning the memories (RAM, ROM, EEPROM) present in the appliance.

Many manufacturers of data communication devices make use of so-called custom chip sets (standard integrated circuits produced in large numbers) or accommodate hardware produced in large numbers and delivered to many manufacturers in a separate housing. The specifications of the manufacturer will, in many cases, describe only the functions desired by the manufacturer. It is therefore possible that (RDS) functionality is present in custom chip sets or hardware which is not made known to the end user.

In the modern information society, knowledge is power. Information is, of course, well protected by means of physical and organizational protection measures of all kinds. Documents may, for example, be seen only by a select group of individuals, after which they are securely stored in the safe. For the purpose of rapid decision-making and refreshing the information situation, consultation will often be made by telephone, in which case use is frequently made of the fax machine to transmit the documents to be discussed to one another. It is here that there is a weak point in the entire security chain. Essentially, the respective documents are made available to third parties, the intention

being precisely to avoid that. Said third parties, who possibly have direct business interests or operate in the world of information brokerage, may acquire possession of valuable information. This may take place even without the owner of the sensitive information even having any indication until it is too late. The industrial spy therefore appears to be very near at hand and works, it is to be noted, together with the individual who has protected his own information with every means.

A fax machine has, for example, RDS functionality, whether this is known to the end user or not, and can thereby be manipulated by a third party. Said third party can ensure, for example, that the respective fax machine responds to certain fax numbers and/or fax identification numbers. During the transmission and/or reception of faxes from/to these fax numbers, the fax machine will transmit, for example, an additional copy to the fax number specified by said third party. The user of the fax machine does not, however, notice anything in this case because the visual and audible signals can be switched off, the so-called fax through-connection number does not have to figure in the list of fax through-connection numbers and even the fax log does not have to report this operation. If necessary, a copy of the fax involved is transmitted only during the night hours when no-one is present in the company.

In the case of a network fax or a modem fax incorporated in a network system within a company, it is conceivable that a third party obtains access via said fax or said modem to the network system. As a result, it might be possible also to extract information in the manner mentioned above from the network system, which is believed to be safe.

The object of the present invention is to provide a method and a device for protecting data communication traffic in order to prevent third parties being able to make unnoticed use of functionality present in a communication station.

According to the invention, the object is achieved by means of a method of the type defined in the introduction, characterized by the steps of the comparison of the data protocol with at least one standardized protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station.

Repetitions of commands, or certain combinations of commands, which each belong per se to the standardized protocol but do not lead to normal, effective data communication traffic, are deemed not to belong to the standardized protocol. Specifically, it is possible that such

repetitions or combinations of commands are used to switch on certain RDS functionality.

Before a fax machine, for example, can proceed to the reception and/or transmission of documents, the appliances at both ends of the communication link have to inform one another about the status they are in. After this so-called "handshake" procedure, the information exchange is mutually adapted. Both appliances are now ready and will carry out the desired task. This procedure and the information exchange proceeds according to internationally specified standards, also referred to as protocols, which are specified in part in the so-called ISO, ETSI and ANSI standards or in the ITU regulations. Before, during or after the "handshake" procedure, a check can take place on the presence of certain RDS functionality. To use RDS functionality, a manufacturer will use protocols which are not (entirely) incorporated in the standards. This means that the use of a so-called exotic protocol can indicate the use of RDS functionality. It indicates in any case that the other party is not adhering to the standard protocols. The negation of the standard indicates that the link made is being used in a manner other than that which the user intended.

As a result of using the method according to the invention, an attempt of a third party to switch on (concealed) RDS functionality from the outside will be unsuccessful, as a result of which the probability that information can leak out via the communication equipment used becomes substantially smaller.

Because, according to the invention, the data protocol is compared with standardized protocols, the method according to the invention can be used worldwide.

In an embodiment of the method according to the invention, the user of a communication station is warned if it emerges during the comparison of the data protocol that the latter does not belong to a known standardized protocol. As a result, the user is warned of an attempt of a third party to manipulate his communication station, whereupon the user can take direct action.

In a further embodiment of the method according to the invention, the link is interrupted if it emerges during the comparison of the data protocol that the latter does not belong to a standardized protocol. This has the result that any attempt to manipulate the communication station by a third party will be unsuccessful.

In a preferred embodiment of the method according to the

invention, after ascertaining that the data protocol does not belong to a certain standardized protocol, a data file containing data of the data communication traffic and the second communication station is prepared. As a result of recording said data, the user is enabled to obtain as complete a picture as possible of the user of the second communication station, after which appropriate measures can be taken.

Another aspect of the invention provides a device suitable for carrying out the method according to the invention. For this purpose, the device is provided with memory means for storing data characteristics of a standardized protocol and comparison/forwarding means for the comparison of the stored data characteristics with the data protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station.

With the device according to the invention, it is possible to use the abovementioned method in a data communication environment. An advantage of the device according to the invention is that the user can determine himself, regardless of the brand and type of appliance, whether RDS functionality is permitted. Because the device can be used separately from the local communication station, there is no need to pay attention to any RDS functionality present when purchasing the local communication station.

As a result of the small number of components required, it is possible to manufacture the device in a compact, lightweight and robust form and to adapt it to the situation in which it is used. Furthermore, the operation and the connection of the device are simple.

Preferably, the memory means are designed as a ROM memory. As a result, it is impossible for the contents of the memory means to be manipulated during use, but it is still simple to adapt the device to the latest standardized protocols by replacing the ROM memory.

In an embodiment of the device, the device furthermore comprises warning means. If data is detected of which the data protocol does not comply with the at least one standardized protocol, the user is warned, for example by visual and/or audible warning means. As a result, the user will always be warned if an attempt is made to manipulate the first communication station, even if an attempt is made in these circumstances to switch off indications of the first communication station.

A further embodiment of the device according to the invention comprises display means linked to the comparison/forwarding means, the

display means displaying data relating to the data communication traffic and the second communication station which are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. This can be implemented, for example, as a display screen on the device itself.

As an addition, the device can be provided, in a further embodiment, with input means linked to the comparison/forwarding means for inputting commands relating to the display of the data.

An alternative embodiment of the invention is to provide it with interface means instead of the display means and/or the input means. Said interface means ensure the exchange of data relating to the data communication traffic and the second communication station with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. Said processing device may be, for example, a computer with which the data are processed further and can be displayed.

By means of the display of said data, the user is enabled to obtain as complete a picture as possible of the attempt to manipulate the local communication station, after which appropriate measures can be taken.

According to an embodiment of the invention, the device can be integrated with the local communication station.

The method and the device according to the invention will now be explained further by reference to the drawings.

Figure 1 shows a diagram of an embodiment according to the invention; and

Figure 2 shows a flow chart of the method according to the invention.

Figure 1 shows a diagram of a preferred embodiment according to the invention in which the device 10 for protecting data communication traffic is linked to a first communication station 11 and a second communication station 12. The device 10 comprises comparison/forwarding means 15 which can communicate during operation both with the first communication station 11 and the second communication station 12. The device 10 furthermore comprises memory means 14 linked to the comparison/forwarding means 15. In the preferred embodiment of the invention shown, the device 10 furthermore comprises warning means 16, display means 17 and input means 18, all linked to the

comparison/forwarding means 15. The communication stations 11 and 12 may be, for example, fax or copying machines provided with an RDS functionality.

In the memory means 14, the characteristics of the data communication are stored according to at least one standardized protocol. The comparison/forwarding means 15 serve to compare the data protocol of data which the second communication station wishes to dispatch to the first communication station 11 and to forward only data of which the data protocol complies with the at least one standardized protocol to the local communication station 11.

In the preferred embodiment shown, the device 10 also comprises warning means 16, which give a warning after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. The figure indicates that the warning means 16 are implemented as a warning lamp. However, it is possible to use other visual or audible warning means for this purpose.

In the preferred embodiment of the invention shown, the device 10 also comprises display means 17 for displaying data relating to the data communication traffic and the second communication station 12 which have been stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. Furthermore, the device comprises input means 18 for inputting commands relating to the display of the data. It is possible, for example, to input commands to display only a certain portion of the data on the display means.

In an embodiment of the invention not shown, the device 10 comprises, instead of the display means 17 and input means 18, interface means which can be linked to an external processing device. This processing device may be, for example, a computer with which the data can be processed further, stored and displayed.

Figure 2 shows the flow chart of the method according to the invention. The method begins with the reception of data from the second communication station 12 in block 1. In decision block 2, the data protocol of the data received in block 1 is compared with the standardized protocol. If the data protocol complies with the at least one standardized protocol, the data is forwarded to the first communication station 11 in forwarding block 3. The method then returns to block 1 to check the further data received.

If the data protocol does not comply with the at least one

standardized protocol, the method continues the procedure in warning block 4, in which the user is warned. The following step in the procedure comprises the interrupt block 6, in which the link to the second communication station is interrupted. In a preferred embodiment of the method according to the invention, in block 5, a data file is stored in which data of the data communication traffic and the second communication station are stored in parallel with warning block 4 and interrupt block 6.

Using the method and device shown in the figures for protecting data communication traffic, an attempt of a third party to switch on (concealed) functionality from the outside will be unsuccessful, as a result of which the probability that information can leak out via the communication equipment used becomes appreciably smaller.

As a result of warning the user and recording data relating to the data communication traffic and the second communication station 12, the user is enabled to obtain as complete a picture as possible of the user of the second communication station, after which appropriate measures can be taken.

An advantage of the device described is that the user can determine himself, regardless of the brand and type of appliance whether RDS functionality is permitted. Because the device can be used separately from the first communication station, there is no need to pay attention to any RDS functionality present when purchasing the first communication station. Of course, the device 10 can also be physically incorporated in the first communication station 11. In that case, the comparison/forwarding means 15 can form an integral component of a processor present in the first communication station 11.

As a result of the comparison of the data protocol of the received data with standardized protocols, the method according to the invention can be used worldwide.

As a result of the small number of components required, it is possible to manufacture the device in a compact, lightweight and robust form and to adapt it to the situation in which it is used. Furthermore, the operation and the connection of the device are simple.

If the memory means are designed as a ROM memory, it is impossible for the contents of the memory means 14 to be manipulated during use, but it is still simple to adapt the device to the latest standardized protocols by means of replacing the ROM memory.

Although the device has been described for the protection of

data communication traffic between two communication stations, it is, of course, also possible to protect the data communication traffic between a plurality of communication stations, such as, for example, in a network environment.

CLAIMS

1. Method for protecting data communication traffic between a first communication station (11) and a second communication station (12), in which the data is dispatched according to a data protocol from the second to the first communication station, characterized by the following steps:

(i) the comparison of the data protocol with at least one standardized protocol;

(ii) the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station (11).

2. Method according to Claim 1, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a warning is generated.

3. Method according to Claim 1 or 2, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, the data communication traffic is interrupted.

4. Method according to one of the preceding claims, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a data file containing data of the data communication traffic and the second communication station (12) is stored.

5. Device for protecting data communication traffic between a first communication station (11) and a second communication station (12), data being dispatched according to a data protocol from the second to the first communication station, characterized in that the device (10) comprises:

- memory means (14) in which data characteristics of at least one standardized protocol are stored;

- comparison/forwarding means (15) for the comparison of the stored data characteristics with the data protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station (11).

6. Device according to Claim 5, characterized in that the device furthermore comprises warning means (16) linked to the comparison/forwarding means (15) which give a warning after it has emerged during the comparison of the data protocol that it does not

belong to the at least one standardized protocol.

7. Device according to Claim 5 or 6, characterized in that the device furthermore comprises display means (17) linked to the comparison/forwarding means (15), the display means (17) displaying data relating to the data communication traffic and the second communication station (12), which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

8. Device according to Claim 7, characterized in that the device furthermore comprises input means (18) linked to the comparison/forwarding means (15) for inputting commands relating to the display of the data.

9. Device according to Claim 5 or 6, characterized in that the device comprises interface means for exchanging data relating to the data communication traffic and the second communication station (12) with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

10. Device according to one of Claims 5 to 9, characterized in that the device (10) is integrated in the first communication station (11).

Fig 1

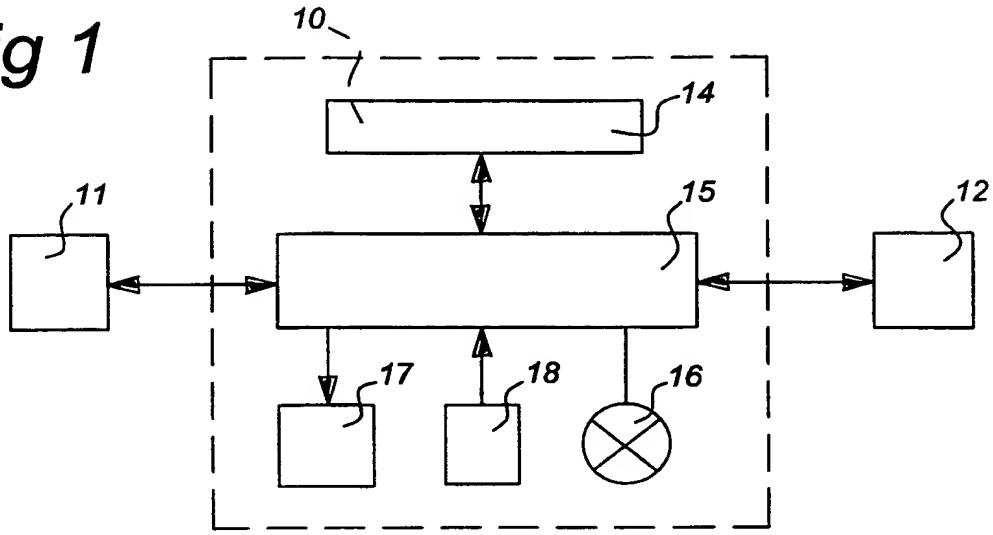
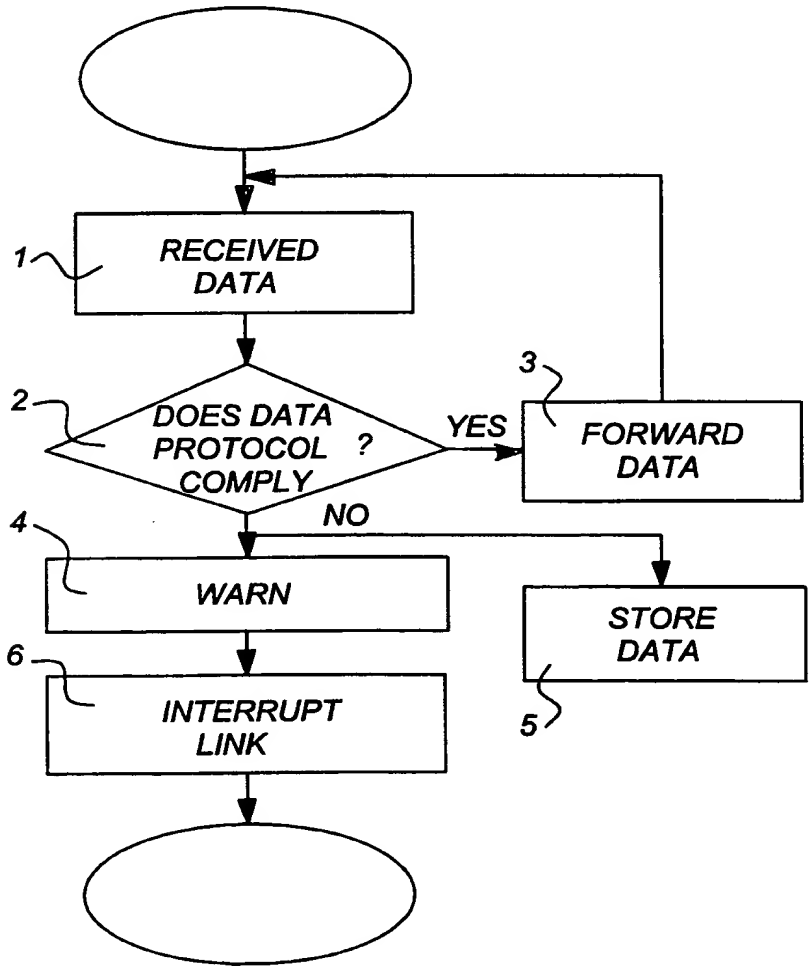

10
14
11
15
12
17
18
16

Fig 2


RECEIVED DATA
1
DOES DATA PROTOCOL COMPLY ?
2
YES
3
FORWARD DATA
NO
4
WARN
STORE DATA
5
6
INTERRUPT LINK

INTERNATIONAL SEARCH REPORT

Inte Application No
PCT/NL 98/00581

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06 G03G15/00 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04M G03G H04N G06G G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 5 124 984 A (ENGEL FERDINAND) 23 June 1992 see abstract see column 1, line 12-66 see column 2, line 38 - column 5, line 7 see column 6, line 35-55 see column 8, line 30 - column 12, line 18 see figures 1,2	1-3,5 4,6,9,10
Y A	US 5 675 510 A (COFFEY STEVEN R ET AL) 7 October 1997 see abstract see column 2, line 34 - column 3, line 5	4,9 7,8
Y	US 5 057 941 A (MORIYA DAISUKE) 15 October 1991 see abstract see column 2, line 7-23	6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 March 1999	17/03/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lievens, K

1

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 245 658 A (BUSH GEORGE ET AL) 14 September 1993 see column 5, line 39 - column 6, line 15 ---	10
A	US 5 337 349 A (FUROHASHI IKUKO ET AL) 9 August 1994 see abstract see column 1, line 55 - column 2, line 3 ---	7,8
A	US 5 226 074 A (HAN SANG-HO) 6 July 1993 see abstract see column 1, line 33-44 ---	1-10
A	EP 0 509 525 A (CANON KK) 21 October 1992 see abstract see column 2, line 44 - column 3, line 20 ---	1-10
A	GB 2 265 158 A (TOKYO SHIBAURA ELECTRIC CO) 22 September 1993 see abstract see page 1, line 1 - page 3, line 12 ---	10
A	US 4 805 206 A (BEOM-CHAE JEONG) 14 February 1989 see abstract see column 4, line 40-49 -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int[illegible] Application No
PCT/NL 98/00581

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5124984 A	23-06-1992	WO 9203001 A	20-02-1992
US 5675510 A	07-10-1997	AU 701813 B	04-02-1999
		AU 6273996 A	30-12-1996
		CA 2223919 A	19-12-1996
		DE 843946 T	04-03-1999
		EP 0843946 A	27-05-1998
		JP 10510647 T	13-10-1998
		NO 975728 A	06-02-1998
		WO 9641495 A	19-12-1996
US 5057941 A	15-10-1991	JP 3010448 A	18-01-1991
		DE 69025648 D	11-04-1996
		DE 69025648 T	02-10-1996
		EP 0401804 A	12-12-1990
US 5245658 A	14-09-1993	NONE	
US 5337349 A	09-08-1994	JP 5145658 A	11-06-1993
		JP 5145694 A	11-06-1993
US 5226074 A	06-07-1993	DE 4108127 A	05-03-1992
		FR 2666469 A	06-03-1992
		GB 2249457 A,B	06-05-1992
		JP 2525084 B	14-08-1996
		JP 6090317 A	29-03-1994
EP 0509525 A		NONE	
GB 2265158 A	22-09-1993	JP 5317571 A	03-12-1993
		KR 9701016 B	25-01-1997
US 4805206 A	14-02-1989	NONE	